FOR 1

(12) UK Patent Application (19) GB (11) 2 079 109 A

(21) Application No 8119018
(22) Date of filing
19 Jun 1981
(30) Priority data
(31) 160985
(32) 19 Jun 1980
(33) United States of America (US)
(43) Application published
13 Jan 1982
(51) INT CL³ H04L 9/04
(52) Domestic classification
H4P DCSP
H4R 17B 17D 17T CST
(56) Documents cited
GB 1318921
EP 0002578A
(58) Field of search
H4P
(71) Applicant
Oak Industries Inc
16935 West Bernardo Drive
Rancho Bernardo
California
United States of America
(72) Inventors
Leo Isaac Bluestein
Paul Ed Crandell
David Anderson Drake
Leo Jedynak
Larry Wallace Simpson
(74) Agents
Marks & Clerk
57-60 Lincoln's Inn Fields
London
WC2A 3LS

(54) A system for enciphering and deciphering digital signals

(57) A transmitter for enciphering information bearing RF signals in digital form has a data enciphering circuit 12 which utilizes a first key common to all receivers. The first key is charged by a key generator 14 of the transmitter, which sends an individual message to each receiver, each message being itself enciphered in a second key which is peculiar to only one receiver or small group of receivers and which message includes a change of the first key. The key generator 14 is controlled by an initiate new key circuit 20. At each receiver there is a comparator responsive to the correct address in a key change message which will thereafter permit the deciphering of the key change message in the key peculiar to that particular receiver or small group of receivers. The new first key is then used at the receiver to decipher subsequent information bearing messages.

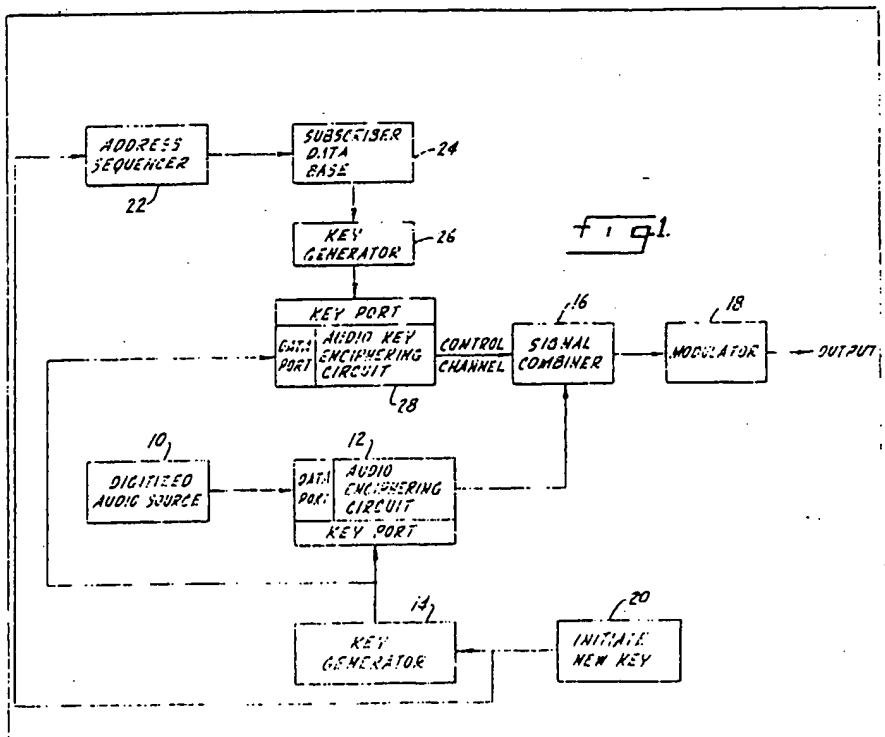

fig 1.

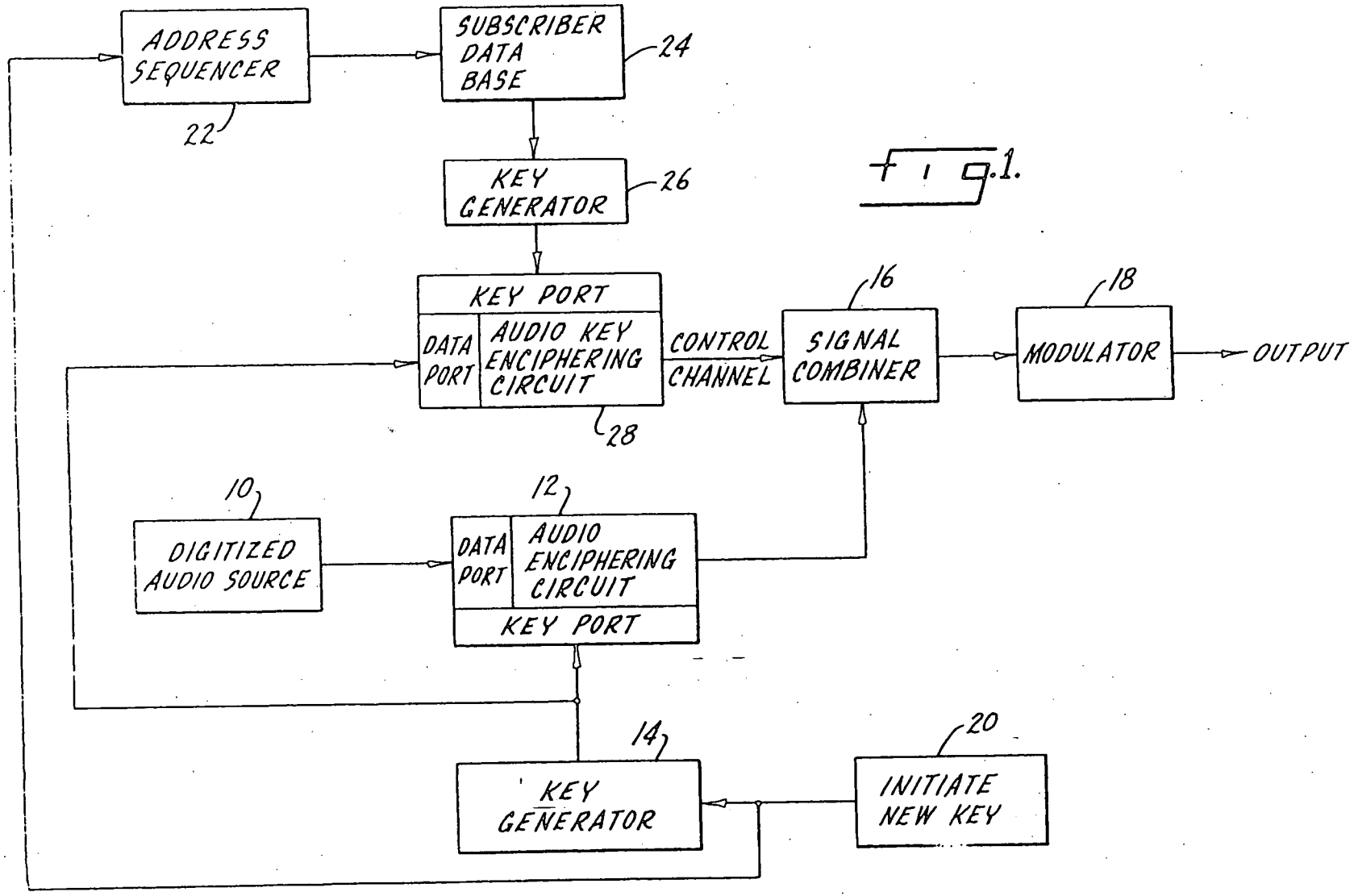

fig. 1.

1 / 2

2979109

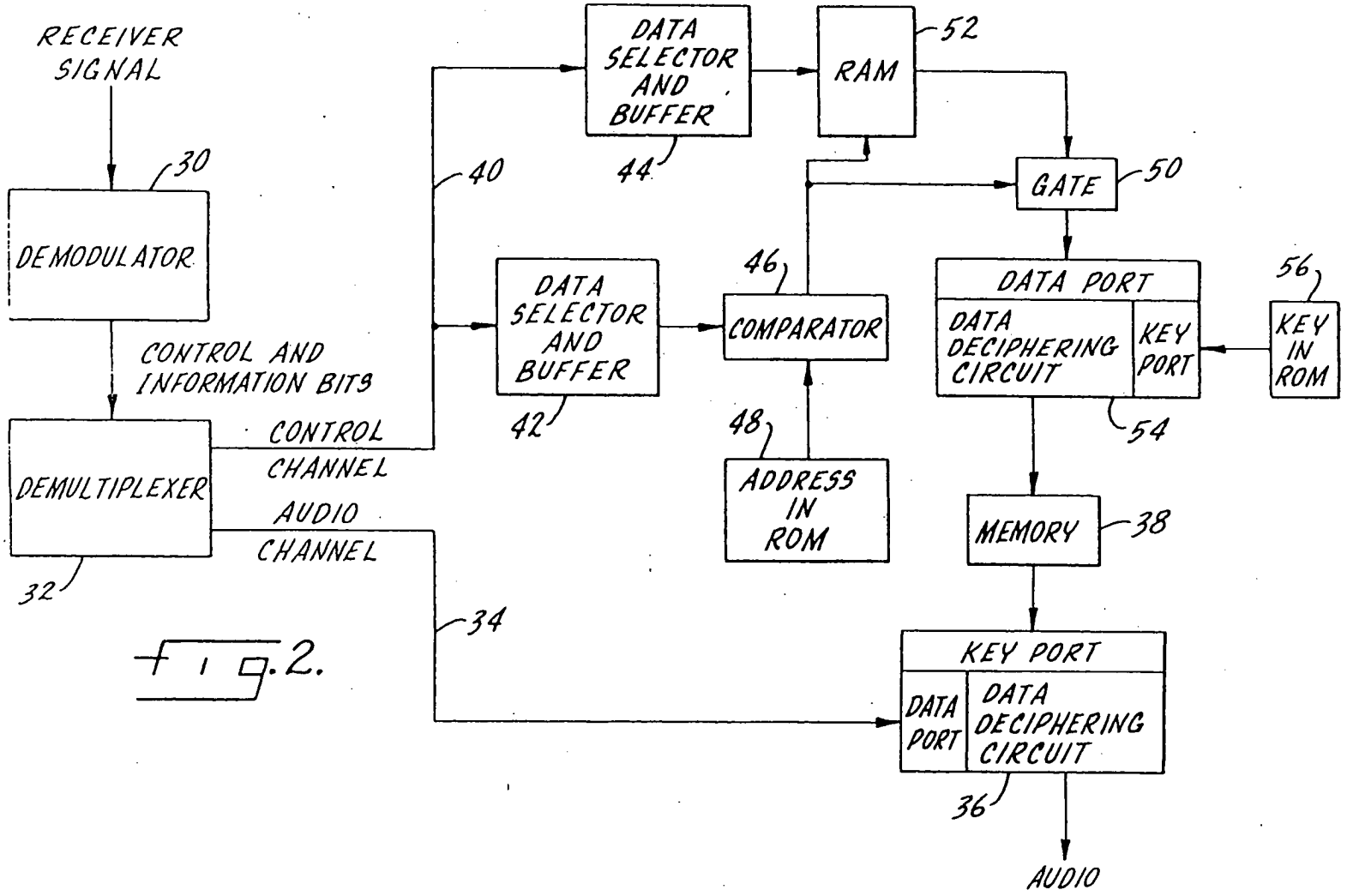

fig. 2.

SPECIFICATION

A system for enciphering and deciphering digital signals

The present invention relates to means for enciphering or encripting messages in digital format and which may have particular application to the communications industry. The invention is particularly applicable to the enciphering and deciphering of audio signals, for example those usable in some form of subscription radio or cable format. The invention has substantially wider application and may be usable with the enciphering of video signals, for example, for a subscription television broadcast or for cable television, and also has utility in the area of satellite transmissions, both of audio type signals, video signals and other forms of information, such as data which can be transmitted in digital form.

According to one aspect of this invention, there is provided a transmitter for enciphering digital information bearing signals, comprising means for using a first key to encipher the digital signals, means for transmitting the enciphered digital signals to a plurality of receivers, means for changing said first key, means for enciphering, in a second key, an information message as to the change in said first key, and means for transmitting to said plurality of receivers, said message in said second key as to the change in said first key.

According to another aspect of the invention, there is provided a receiver for deciphering enciphered digital information bearing signals, comprising first deciphering means responsive to a first key for deciphering said digital signals, means for changing said first key including second deciphering means responsive to a message enciphered in a second key and which includes a change in said first key.

The invention provides an enciphering system which has two levels of security, the first level providing enciphering of the information bearing signals, with the second level of security being used to encipher changes in the code or key for deciphering the information bearing messages at the first level of security.

Preferably, the second level of security includes a separate independent enciphering key for each receiver in the system.

However, the principles disclosed are equally applicable with a separate deciphering key for each small group of receivers. Use of the term receiver should be understood to include a small group of receivers. What is important is not to use a deciphering key common to more than a small number of individual subscribers.

The transmitter may be arranged to regularly broadcast or transmit information bearing messages in enciphered form in a particular key, which may be changed on a periodic basis.

The invention is illustrated diagrammatically in the accompanying drawings wherein:–

Figure 1 is a block diagram of a transmitter according to this invention; and

Figure 2 is a block diagram of the receiver according to this invention and usable with the transmitter of Fig. 1.

As indicated above, the two level security enciphering concept disclosed herein has application in a wide variety of communication systems. It is usable in satellite transmission, subscription television, subscription radio, cable systems and various forms of data transmission. The following description will be particularly applicable to the enciphering of digital audio information, although quite obviously, when considering the above comments, the invention should not be so limited.

In Fig. 1 a source of audio information in digital form is indicated at 10 and is connected to a data enciphering circuit 12 which may, for example, utilize a Fairchild 9414 as the basic integrated circuit for enciphering the digitized audio information. The sourc of digital audio information is connected to the data part of enciphering circuit 12. A key generator 14 is connected to the key port of enciphering circuit 12 and will provide the key use in enciphering the digitized audio information. Thus, the output from enciphering circuit 12 is the digitized audio information enciphered in a particular key referred to hereinafter as the first key.

The output signal from circuit 12 will pass to a signal combiner 16 and then to a modulator 18 which will transmit the information in a form appropriate for the particular medium, whether it be broadcast, cable or satellite.

As indicated above, the first key will be changed on some type of regular basis to provide a more secure system. An initiate key change circuit is indicated at 20 and will effect the formation of a new key by key generator 14. The new key will then be applied in block 12 for the enciphering of the ditigized audio information. The initiate new key signal is also applied to an address sequencer 22 which will effect a search of valid subscriber addresses stored in a random access memory or subscriber data base 24. The subscriber list may not be searched in any particular order, as what is important is to insure that each subscriber whose address is still valid will be addressed any time there is a key change.

Connected to the subscriber data base 24 is a key generator 26 which may be in the form of a read only memory or ROM and which will include a separate independent key for every subscriber in the overall system. The output from key generator 26 is connected to a key enciphering circuit 28 which will receive at its data port the new key from key generator 14. In this connection key generator 14 may be a

random number generator which creates independent non-repetitive keys. The new key provided at the data port will be enciphered by the series of keys provided from key generator 26 with the result that each message will include an address and an enciphered new key with the enciphering being done in a second key which is different for each receiver. This message is the output from circuit 28 and is connected to the signal combiner for subsequent transmission as described above. Thus, every time there is to be a change in the first key for enciphering the information bearing signals, this change in key itself is enciphered in a message which includes an address and the first key enciphered in a second key with the second key being peculiar to only a single receiver.

Referring to the receiver shown in Fig. 2, the information bearing and key change messages described in connection with Fig. 1 are received at a demodulator 30 which provides the control and information bits to a demultiplexer 32. There are two outputs from demultiplexer 32. One output designated the audio channel at 34, is connected to a data deciphering circuit 36 which has a data port and a key port. The enciphered information bearing signal will be provided at the data port and the output from data encipher circuit 36 will be the audio information in usable form.

A memory 38 which will contain the particular key or first key usable at a specific time is connected to the key port of data deciphering circuit 36 and thus will provide the means for deciphering the coded information bearing signals. Again, the particular integrated circuit for the data deciphering circuit may be a Fairchild 9414 suitably connected for deciphering.

The second output from the demultiplexer 32 is a control channel indicated at 40 which is connected to a first data selector and buffer amplifier circuit 42 and a second similar circuit 44. Circuit 42 will select the address portion of a control message, whereas, circuit 44 will select the message portion. Circuit 42 is connected to a comparator 46 wherein the address portion of the message is compared with a hard-wired address in a ROM 48. Assuming there is a valid comparison and thus that the message is for that particular receiver; there will be an output from comparator 46 to a gate 50 and to a random access memory (RAM) 52. RAM 52 will receive the enciphered key portion of the message from data selector 44 with this key being temporarily stored in the RAM. When an appropriate signal is received from comparator 46, the enciphered message in the RAM will be passed through gate 50 to the data port of a second data deciphering circuit 54. The key port of data deciphering circuit 54 is connected to a ROM 56 which will have a hard-wired key peculiar to a particular receiver Thus, the enciphered new key, or first key, will be received at the data port of circuit 54 and the key for deciphering such message will be received at the key port from ROM 56. Again, circuit 54 may utilize the above-described integrated circuit or one of like kind and quality. The output from circuit 54 will be the deciphered new first key which is stored in memory 38 so that subsequent data bearing messages may be deciphered.

To summarize, the two level security system disclosed herein utilizes a first key to encipher information bearing messages in digital form. The first key will be changed on either a regular or random basis, depending upon the security safeguards necessary in the particular communications environment. When there is to be a change in the first key, the new first key is itself enciphered in a message which is peculiar to each individual receiver or to a small group of subscriber receivers as described above. Such message will include the address of a receiver and the first key enciphered in a code peculiar to that particular receiver. Thus, there will be a series of such messages, one for each receiver in the system. At the receiver the enciphered first key will be deciphered by the second key peculiar to that receiver. The deciphered first key will then be utilized in deciphering subsequent information bearing digital messages.

Whereas the preferred form of the invention has been shown and described herein, it should be realized that there may be many modifications, substitutions and alterations thereto.

CLAIMS

1. A transmitter for enciphering digital information bearing signals, comprising means for using a first key to encipher the digital signals, means for transmitting the enciphered digital signals to a plurality of receivers, means for changing said first key, means for enciphering, in a second key, an information message as to the change in said first key, and means for transmitting to said plurality of receivers, said message in said second key as to the change in said first key.

2. A transmitter according to claim 1, wherein in said second key is different for each of said plurality of receivers.

3. A transmitter according to claim 1, wherein said information message includes an address for each of said plurality of receivers, with said second key being different for each of said plurality of receivers.

4. A receiver for deciphering enciphered digital information bearing signals, comprising first deciphering means responsive to a first key for deciphering said digital signals, means for changing said first key including second deciphering means responsive to a message enciphered in a second key and which includes a change in said first key.

5. A receiver according to claim 4 including address means responsive to an address portion of said key change message for enabling said second deciphering means.

6. A receiver according to claim 4, wherein said second deciphering means is responsive to a key peculiar to only one receiver.

7. A transmitter for enciphering digital information bearing signals substantially as hereinbefore described with reference to Fig. 1 of the accompaying drawings.

8. A receiver for deciphering enciphering digital information bearing signals substantially as hereinbefore described with reference to Fig. 2 of the accompaning drawings.

Printed for Her Majesty's Stationery Office
by Burgess & Son (Abingdon) Ltd.—1982.
Published at The Patent Office, 25 Southampton Buildings,
London, WC2A 1AY, from which copies may be obtained.